IT SECURITY REQUIREMENTS FOR CONTRACTING OFFICIALS AND CONTRACTING OFFICER REPRESENTATIVES

Contracting Officials – individuals with specific authority to process and recommend or specifically obligate the Government; includes Purchasing Agents, Contract Specialists and Contracting Officers (including program officials with Delegated Procurement Authority).

Contracting Officer Representatives – individuals with specific authorities delegated from the Contracting Officer to oversee performance and assist with administration of NOAA's contracts; includes Contracting Officer Technical Representatives (COTRs), Alternate and/or Assistant COTRs, and Point of Order Contact.

DOC Clauses 1352.239-73, Security Requirements for Information Technology Resources, and 1352.239-74, Security Processing Requirements for Contractor/Subcontractor Personnel for Accessing DOC Information Technology Systems, must be included in all DOC solicitations and contracts for services.

RESPONSIBILITIES:

Contracting Officials

Pre-solicitation:

1. Determine whether 1352.239-73 and 1352.239-74 are applicable to the contract by determining whether the contractor will have access to DOC sensitive information, or whether the contractor's systems interconnect to the DOC network.

2. Working with COR, determine appropriate risk level (1352.239-74)

3. Incorporate clauses in solicitation

4. Identify specific deliverables in Section F of the solicitation.

Pre-award:

1. Ensure that clauses are included.

2. Ensure that all required deliverables are identified and due dates established.

3. Determine, in coordination with the COR, the appropriateness of allowing interim access to DOC IT systems pending favorable completion of a pre-employment check.

4. Ensure Contractor understanding of the IT Security Requirements specific to the contract.

Post-Award:

1. Provide formal acceptance of IT Security Plan (SP) and Certification and Accreditation Package (C&A).

2. Take appropriate action, in consultation with COR, Office of General Counsel (OGC), and DOC Office of Security (OSy), regarding any negative or questionable responses to personnel screening forms.

3. Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, adherence to accepted SP and C&A, including appropriate termination activity as appropriate.

Contracting Officer Representatives

Pre-solicitation:

Working with assigned contracting official, determine appropriate risk level and provide formal determination of that risk level with

submission of the acquisition request to the assigned acquisition office.

Post-Award:

1. Receive, evaluate and determine acceptability of contractor's SP and C&A. Requires coordination with DOC OSy (personnel screenings) and DOC/NOAA IT Security Manager/Officer (SP and C&A). Work with Contracting Officer to resolve issues with personnel screenings and SP/C&A. Provide written notice of acceptability of personnel screenings and/or SP/C&A in a timely manner to the Contracting Officer.

2. Work with DOC IT Security Manager/Officer to bring about certification and accreditation of the contractor system.

3. Monitor performance of contractor to ensure compliance with contract terms relating to IT security and with annual IT security awareness training.

4. Assist Contracting Officer with resolution of unacceptable Contractor performance, including termination as appropriate.

5. Ensure that system access is deleted for all contractor employees granted access under the contract by requesting the appropriate system administrator to delete all access rights.

<u>Contractor</u>

1352.239-73 requires the Contractor to:

1. Implement sufficient IT security to reasonably prevent the compromise of DOC IT resources for the contractor's systems that are interconnected with a DOC network, or for DOC systems that are operated by the contractor.

2. Comply with the requirements in the DOC IT Management Handbook.

3. Provide in accordance with the delivery schedule included in the contract, implement and maintain an SP.

4. When contract performance requires that the contractor's systems are interconnected with a DOC network, or that DOC data are stored or processed on the contractor's systems, within 14 days after contract award, submit for DOC approval, a system C&A including the SP and a system certification test plan.

5. Flow provisions of this clause down to all subcontracts under the contract and ensure compliance by the subcontractor(s).

1352.239-74 requires the Contractor to:

1. Submit personnel screening forms to the COR at the inception of the contract and throughout the life of the contract:

a. Pre-employment check required for Contracts designated High Risk, Moderate Risk and for contractor personnel with global access to an automated information system—required before work begins on contract.

b. After favorable pre-employment check is obtained: Submit forms to initiate Background Investigation for High Risk contracts and Minimum Background Investigation for Moderate Risk contracts—required to be submitted within 3 working days of the start of work.

c. For non-IT work designated Moderate Risk, pre-employment checks are not required; submit forms to initiate Minimum Background Investigation within three days after employee's work on the contract begins.

d. Contractor employees on Contracts designated Low Risk are required to have a National Agency Check and Inquiries upon the employees start of work on the contract if expected duration of the

contract exceeds 365 calendar days—must be initiated within 3 working days of the employees' start of work on the contract

e. Contractor employees on contracts designated Low Risk require a Special Agreement Check if duration of the contract is greater than 180 calendar days but less than 365 calendar days—must be initiated within 3 working days of the employees' start of work on the contract.

f. Contractor employees performing work on contracts requiring access to classified information must undergo investigative processing according to DoD National Industrial Security Program Operating Manual--must be granted eligibility for access to classified information prior to beginning work on the contract

2. Within 5 days of contract award, certify to COTR that all contractor employees performing on the contract have completed the annual IT security awareness training.

3. Within 5 days of contract award provide COTR with signed Nondisclosure Agreements.

4. Cooperate and allow access to DOC and Office of Inspector General personnel conducting assessments and investigations.

5. Flow all requirements of Clauses 1352.239-73 and 1352.239-74 to all subcontractors performing on the contract and monitor and ensure their compliance with the requirements of these clauses.

Associated Polices and Resources
- DOC Procurement Memorandum 2003-09
- DOC IT Security Program Policy and Minimum Implementation Standards (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html)
- OAM website
- Executive Order 12931
- DAO 208-2
- DOC Security Manual, Chapter 18 (http://www.osec.doc.gov/osy/)
- DOC Information Technology Management Handbook (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html)
- National Industrial Security Program Operating Manual (http://www.dss.mil/isec/nispom.htm)